Federal Bridge CA Certificate Policy Change Proposal
Change Number: 2003-04

To: Federal PKI Policy Authority

From: FPKIPA Certificate Policy Working Group

Subject: Proposed modifications to the FBCA Certificate Policy

Date: 3 September 2003

Title: FBCA Token Destruction

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), dated 10 September 2002.

Change Advocates Contact Information:

Name: Tim Polk
Organization: NIST
Telephone number: 301-975-3348
E-mail address: tim.polk@nist.gov

Organization requesting change: Federal PKI Policy Authority – Certificate Policy Working Group

Change summary: The FPKIPA CPWG proposes that the requirement stated in Section 4.4.1.2 for the destruction or zeroization of tokens be modifed to address issues of the Certification Authority not having ownership of the device.

Background: The FBCA CPWG meeting with the State of Illinois, Georgia Marsh, on 4 April 2003 that discussed the Generic and Medium policy mapping requirements of the State of Illinois certificate policy to the FBCA CP. This proposed language eliminates a restriction placed on Entity CAs that is unenforceable by the FPKIPA or FBCA OA.

The following insertions in underlined italics are used to depict specific changes.

Specific Changes:

Replace paragraph four of FBCA Section 4.4.1.2:

> For PKI implementations using hardware tokens, a Subscriber ceasing its relationship with an organization that sponsored the certificate shall, prior to departure, surrender to the organization (through any accountable mechanism) all cryptographic hardware tokens that were issued by or on behalf of the sponsoring organization. If a Subscriber leaves an organization and the hardware tokens cannot be obtained from the Subscriber, then all Subscriber's certificates associated with the unretrieved tokens shall be immediately revoked. The token shall be zeroized or destroyed promptly upon surrender and shall be protected from malicious use between surrender and zeroization or destruction.

with the following text:

> For PKI implementations using hardware tokens, revocation is optional if all the following conditions are met:
>
> - the revocation request was not for key compromise;
> - the hardware token does not permit the user to export the signature private key;
> - the Subscriber surrendered the token to the PKI;
> - the token was zeroized or destroyed promptly upon surrender;
> - the token has been protected from malicious use between surrender and zeroization or destruction.
>
> In all other cases, revocation of the certificates is mandatory. Even where hardware tokens are zeroized or destroyed, revocation of the associated certificates is recommended.

Estimated Cost:

The cost of this change to the FBCA CP is nomimal, as cost is associated only the editing, publishing and distribution of the new certificate policy. There is no cost associated with operations or maintenance of the FBCA for this change.

Implementation Date:

This change will be implemented immediately upon approval by the FPKIPA and incorporation into the FBCA CP.

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

There are no prerequisites.

Approval and Coordination Dates:

Date presented to CPWG: September 03, 2003
Date CPWG recommended approval: September 03, 2003
Date Presented to FPKI PA: September 9, 2003
Date of approval by FPKI PA: September 9, 2003